UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/718,064	11/20/2003	Luca Ferri	FR920030006US1	8678

7590 05/29/2007

Jeffrey S. LaBaw
International Business Machines
11400 Burnet Rd.
Austin, TX 78758

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
05/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/718,064	FERRI ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 10/718,064.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Ellen Tran

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to: amendment filed original application filed on 20 November 2003 with acknowledgement of the benefit of a foreign application filed 10 March 2003.

2. Claims 1-19 are pending; claims 1 and 8-19 are independent claims.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-19,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al. U.S. Patent No. 6,367,012 (hereinafter '012) in view of O'Donnell et al. U.S. Patent No. 7,024,689 (hereinafter '689).

As to independent claim 1, "A method of authenticating a digitally encoded product being originated by an entity having at least one authorized subject, the method including the steps of: a client system transmitting a request of authentication of the product to a server system" is taught in '012 col. 7, line 52-67, note the confirmation is in reply to a client system, i.e. browser application call, the 'digitally encoded product' is interpreted to be equivalent to the 'executable file';

"and returning a representation of the certification to the client system" is shown in '012 col. 8, lines 45-63, note providing the recipient computer with a confirmation certification of the received executable code is interpreted equivalent to a 'representation of the certification';

the following is not explicitly taught in '012: **"the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification: certifying that the product originates from the entity using sensitive information of the entity stored on the server system"** however '689 teaches "In one embodiment, the present invention allows subscribers to grant access rights to a client application in a system where a subscriber uses a client application to access a server application. An access site accommodates the granting of access rights, acting as a neutral broker between the client and server applications ... A subscriber navigates to the client application (typically residing at a web site referred to as a client site), and requests features of the client application that implement the server application. This request can be variously made. For example, it can be a selection of a server application based feature that is presented at the client site, part of a more formal registration, and the like. After such a request, the subscriber is taken through steps that allow the subscriber to grant permission to a client application to access the server application. The granted permission can be variously defined. For example, the subscriber may grant permission for a payroll application to access an accounting application. However, the subscriber may not want the payroll application to be able the access certain accounting data. Further, the subscriber may want to require an authorized user to login prior to granting a request to process subscriber data", in col. 2, line 57 through col. 3, line 20. Note the Examiner interprets the 'access site' that acts as a neutral broker to be equivalent to the 'server system'.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system that embeds certification or signatures in a computer program, an executable file, or code to assure is authenticity taught in '012 to include a means to control who has access to the computer programs, executable file, or code. One of ordinary skill in the art would have been motivated to perform such a modification because of the need for subscriber data management see '689 (col. 2, lines 15-49) "One continuing need with online applications is subscriber data management. In the two party transaction model, data management is relatively straightforward. The server application is configured to provide access only to authorized subscribers (users) who sign in through names and passwords. Because the service provider's applications are the only ones that can programmatically access the subscriber's data, there is little or no need for application level data security or management, since it is assumed that the service provider's applications are trusted. Such is not the case in a three party model, where an independent, third party client application is attempting to access a subscriber's data at the service provider ... Third, there is the converse problem of the third party application ensuring that its use by the subscriber on the server data is authorized, that is, that the subscriber is in fact a legitimate subscriber of the server application's functionality and data hosting services. These various distinct types of control and management are currently not met by conventional client-server systems. Thus, while online applications allow great flexibility and other advantages, it would be desirable to allow subscribers improved control over the granting of access rights corresponding to their applications and underlying subscriber data".

As to dependent claim 2, "wherein the step of verifying whether the request is received from an authorized subject includes: comparing an address of the client system

with an indication of authorized addresses stored on the server system" however '689 teaches, "For example, the access site may retain the address of the client site and ensure that the confirmation code is coming from a valid address. Once the confirmation codes have been received, verification 220 involves a comparison of the code sent by the subscriber to the one sent by the client application" in col. 11, lines 4-7. The motivation to combine '012 and '689 is the same as stated above in claim 1.

As to dependent claim 3, "wherein the step of verifying whether the request is received from an authorized subject includes: comparing an identifier of a user logged on the client system with an indication of authorized users stored on the server system" however '689 teaches, "In one embodiment, the subscriber also has the option of associating login security to the set of permissions. This means that before exchanging data two validation tokens must be presented by the client application to the server application. The first validation token is the one described above. It proves that someone has given permission for the client application to request services from the server application. A second validation token indicates that an authorized user has given permission (e.g., logged in) for a particular data exchange to occur. This can be referred to as a user validation token" in col. 3, line 62 through col. 4, line 5. The motivation to combine '012 and '689 is the same as stated above in claim 1.

As to dependent claim 4, "wherein the step of certifying includes: automatically retrieving a private key of the entity stored on the server system, and digitally signing the product using the private key" however '689 teaches "Initially, application developers correspond with the access site to reserve names and receive corresponding certificates for client applications that they develop. These certificates are subsequently used as part of securely

granting access to the server application by the client application. Specifically, the certificate is used to ensure that subsequent communications securely originate from the client application" and "When the subscriber requests client application features that integrate with the server application, the client application gives the subscriber a unique confirmation code .... Preferably, the confirmation code is sent by the client application to the server application using a security mechanism (e.g., SSL) that implements the previously issued certificate. This provides assurance to the server application that the confirmation code has been sent by the client application" in col. 2, line 63 through col. 3, line 3 and col. 3, line 25-41. Note the certificates issued utilize 'private keys'. The motivation to combine '012 and '689 is the same as stated above in claim 1.

As to dependent claim 5, "wherein the step of automatically retrieving the private key includes: calling a signing command passing a password for accessing the private key as a parameter" however '689 teaches, "In one alternative, "login security" can also be associated with a proxy account as described above. Generally, when the login security option is selected the subscriber choose particular users who must login when the client application seeks to access the server application according to the otherwise specified access rights. If login security is enabled, then the server application will later request login credentials, such as a username and password for a particular authorized user, when the client application seeks to access subscriber data through the server application. The login security feature is described further with reference to FIG. 3 below" in col. 11, lines 59 through col. 12, line 3. The motivation to combine '012 and '689 is the same as stated above in claim 1.

As to dependent claim 6, "wherein the step of automatically retrieving the private key includes: calling a signing command with an option causing the import of the private

key from a private configuration memory area of the server system" however '689 teaches, " If login security is enabled for the proxy account, then a login security phase 320 is invoked, to ensure that access by the client application is associated with a request by a particular authorized user. Initially, this involves sending 322 a code indicating that user login is required to the client application. The client application is configured to recognize this code, and to prompt the particular authorized user to browse 324 to the login server (preferably the access site, but could equally be the server application if the server application is directly handling the login security aspect of the proxy account), and to then provide 326 credentials. The communication is in conjunction with the previous presentation of the validation token, which is correlated to the proxy account, which in turn identifies the list of users who may login. The credentials are preferably in the form of a user name and password, although any login credential can be used, including but not limited to a code or key, biometric data, a code that uniquely identifies the authorized user's machine, etc. The access site receives and verifies appropriate credentials corresponding to the proxy account, and then sends 328 a user validation token to the authorized user. Like the account validation token, the user validation token can be any kind of unique code, number or the like. The authorized user sends 330 the user validation token to the client application, which in turn sends 332 it to the access site. Receipt of the user validation token from the client application indicates to the access site that the client application request is associated with the "logged in" authorized user, and thus prompts an indication 340 and corresponding approval of the data exchange through the proxy account" in col. 13, lines 6-36. The motivation to combine '012 and '689 is the same as stated above in claim 1.

As to dependent claim 7, "further including the steps of: the client system invoking a remote command on the server system, the server system verifying whether the remote command is included in a predefined list stored on the server system, the list including at least one remote command for satisfying the request of authentication, and the server system executing the remote command if included in the list" however '689 teaches, "The client site provides web pages for interfacing with potential subscribers. As described above, a subscriber may navigate to a page pertaining to a client application and indicate 210 that he would like to use features of the client application that integrate with the server application. Pursuant to such an indication, an approved subscriber verification phase 208 provides confirmation that a subscriber contacting the server application is a legitimate user of the client application. Particularly, upon receipt of the indication that the subscriber would like to use such features, the client application generates a confirmation code that is sent 212 to the subscriber. The confirmation code can be any unique piece of information, typically dictated by the client application. For example, the confirmation code can be any number or alphanumeric string. The subscriber is also redirected 212 to the access site by a redirect command that directs the subscriber to the access site. The redirect may also include information that specifically directs the user to a particular server application, and may also include information that allows the access site to automatically respond once the subscriber is navigated to the access site" in col. 10, lines 18-38. The motivation to combine '012 and '689 is the same as stated above in claim 1.

As to independent claim 8, "A method of authenticating a software product being originated by an entity having at least one authorized subject, the method including the steps of: a client system transmitting a request of authentication of the product to a server

system" is taught in '012 col. 7, line 52-67, note the confirmation is in reply to a client system, i.e. browser application call, the 'digitally encoded product' is interpreted to be equivalent to the 'executable file';

"and returning the digital signature to the client system" is shown in '012 col. 2, lines 53-61';

the following is not explicitly taught in '012:

"the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification: generating a digital signature of the product using a private key of the entity stored on the server system" however '689 teaches "In one embodiment, the present invention allows subscribers to grant access rights to a client application in a system where a subscriber uses a client application to access a server application. An access site accommodates the granting of access rights, acting as a neutral broker between the client and server applications ... A subscriber navigates to the client application (typically residing at a web site referred to as a client site), and requests features of the client application that implement the server application. This request can be variously made. For example, it can be a selection of a server application based feature that is presented at the client site, part of a more formal registration, and the like. After such a request, the subscriber is taken through steps that allow the subscriber to grant permission to a client application to access the server application. The granted permission can be variously defined. For example, the subscriber may grant permission for a payroll application to access an accounting application. However, the subscriber may not want the payroll application to be able the access certain accounting data. Further, the subscriber may want to require an authorized user to login prior to granting a request to process

subscriber data", in col. 2, line 57 through col. 3, line 20. Note the Examiner interprets the 'access site' that acts as a neutral broker to be equivalent to the 'server system'. Also note the certificates issued utilize 'private keys'.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system that embeds certification or signatures in a computer program, an executable file, or code to assure is authenticity taught in '012 to include a means to control who has access to the computer programs, executable file, or code. One of ordinary skill in the art would have been motivated to perform such a modification because of the need for subscriber data management see '689 (col. 2, lines 15-49) "One continuing need with online applications is subscriber data management. In the two party transaction model, data management is relatively straightforward. The server application is configured to provide access only to authorized subscribers (users) who sign in through names and passwords. Because the service provider's applications are the only ones that can programmatically access the subscriber's data, there is little or no need for application level data security or management, since it is assumed that the service provider's applications are trusted. Such is not the case in a three party model, where an independent, third party client application is attempting to access a subscriber's data at the service provider ... Third, there is the converse problem of the third party application ensuring that its use by the subscriber on the server data is authorized, that is, that the subscriber is in fact a legitimate subscriber of the server application's functionality and data hosting services. These various distinct types of control and management are currently not met by conventional client-server systems. Thus, while online applications allow great flexibility and other advantages, it

would be desirable to allow subscribers improved control over the granting of access rights corresponding to their applications and underlying subscriber data".

As to independent claim 9, this claim is directed to a computer program processing the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 10, this claim is directed to a program product processing the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 11, this claim is directed to a computer program product processing the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 12, this claim is directed to a program product processing the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 13, this claim is directed to a computer program performing the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 14, this claim is directed to a program product processing the method of claim 1; therefore it is rejected along similar rationale.

As to independent claims 15-19, these claims are directed to a data processing structure processing the method of claim 1; therefore they are rejected along similar rationale. Note the Examiner interprets '689 and '012 teaching that their inventions apply to at least one application, residing in at least one client system, with at least one server or access site as well as at least one memory.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
23 May 2007